PATENT ABSTRACTS OF JAPAN

(11)Publication number : 63-273980
(43)Date of publication of application : 11.11.1988

(51)Int.Cl. G06K 17/00
G06F 15/21
H04L 9/00

(21)Application number : 62-108510
(22)Date of filing : 01.05.1987

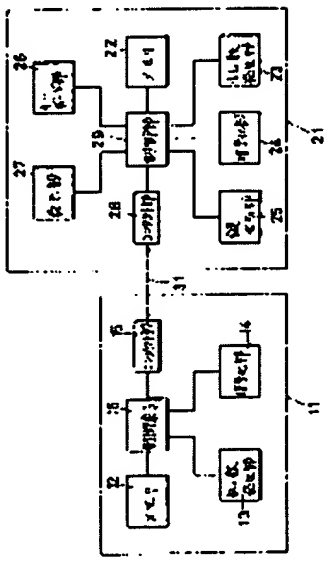
(71)Applicant : TOSHIBA CORP
(72)Inventor : KAWAGISHI TOSHIYUKI

(54) MUTUAL CONFIRMATION SYSTEM

(57)Abstract:

PURPOSE: To prevent the forgery of 1st and 2nd electronic devices by securing a communication enable state between both electronic devices only when they decide the propriety of communication after confirming their states with each other.

CONSTITUTION: The random number generating parts 13 and 23 are provided to an IC card 11 (1st electronic device) and a terminal equipment 21 (2nd electronic device) for production of different random numbers. At the same time, the ciphering parts 14 and 24 are provided to the card 11 and the equipment 21 for production of outputs which are well-definedly decided to the same optional input. Then the random number data produced by the card 11 and the equipment 21 are transferred to each other and the outputs decided well-definedly to the received random number data are produced and sent to each other. Thus the propriety of the remote side is judged from the contents of the received output. The communication is possible between the card 11 and the equipment 21 only when they judge the propriety with each other. Thus it is possible to prevent the forgery of the card 11 and the equipment 21.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Reference 1

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　昭63-273980

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開 昭和63年(1988)11月11日
G 06 K 17/00		S-6711-5B	
G 06 F 15/21	340	Z-7230-5B	
H 04 L 9/00		A-7240-5K	審査請求 未請求 発明の数 1 (全6頁)

㊹発明の名称　相互認証方式

㉑特　願　昭62-108510

㉒出　願　昭62(1987)5月1日

㉗発明者　川岸　敏之　神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内

㉑出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地

㉔代理人　弁理士　鈴江　武彦　外2名

明　細　書

1．発明の名称

相互認証方式

2．特許請求の範囲

（1）第1の電子装置と、この第1の電子装置との間で通信可能な第2の電子装置とからなり；

前記第1の電子装置は、第1の乱数データを発生する第1の手段と、所定のアルゴリズムにより任意の入力に対して一意に定まる出力を形成する第2の手段とを具備し；

前記第2の電子装置は、第2の乱数データを発生する第3の手段と、前記第2の手段のアルゴリズムと同一のアルゴリズムにより任意の入力に対して一意に定まる出力を形成する第4の手段とを具備し；

かつ前記第1の電子装置と第2の電子装置とが通信を行なう際；

前記第1の電子装置は、前記第1の手段から第1の乱数データを発生させて前記第2の電子装置に送り、前記第4の手段によって前記第1の乱数データにより一意に定まる出力を前記第2の電子装置から返信させ、その返信内容から前記第2の電子装置の正当性を判断する第5の手段を具備し；

前記第2の電子装置は、前記第3の手段から第2の乱数データを発生させて前記第1の電子装置に送り、前記第2の手段によって前記第2の乱数データにより一意に定まる出力を前記第21電子装置から返信させ、その返信内容から前記第1の電子装置の正当性を判断する第6の手段を具備し；

前記第5の手段および第6の手段によって前記第1の電子装置および第2の電子装置が互いに相手を正当と判断したときのみ通信可能とすることを特徴とする相互認証方式。

（2）前記第1の電子装置は固有の識別情報を有していて、前記第2の手段および第4の手段の入力として少なくともこの識別情報および前記乱数データを用いることを特徴とする特許請求の範囲第1項記載の相互認証方式。

（3）前記所定のアルゴリズムは暗号化アルゴリズムであることを特徴とする特許請求の範囲第

1項記載の相互認証方式。

（4）前記第1の電子装置はICカードであることを特徴とする特許請求の範囲第1項記載の相互認証方式。

（5）前記第2の電子装置は前記第1の電子装置に対する上位装置であることを特徴とする特許請求の範囲第1項または第4項記載の相互認証方式。

3．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

本発明は、たとえば電子的な手段で取引を行なうシステム、すなわちICカードを用いたキャッシュレスショッピングシステムやクレジットシステムにおいて、ICカードとその端末装置との相互認証やICカードとその発行装置との相互認証を可能にする相互認証方式に関する。

（従来の技術）

最近、銀行のキャッシュカードやクレジットカードの利用機会が急激に増えている。それに伴い、カードを悪用した犯罪も増加する傾向があり大きな問題となっている。これにより、高いセキュリティを持つICカードが非常に注目を集めている。

ICカードは、データを内部のメモリに記憶するため、データへのアクセス制御を容易にかけることができる。また、ICカードは、制御素子（CPU）を内蔵するため、データの暗号化や暗証情報の内部でのチェックといった積極的なセキュリティ機能を実現することも可能である。

しかしながら、ICカードを用いたシステムにおいて、ICカードの偽造やICカード用端末装置の偽造に対して対策がなされておらず、このためICカードの偽造や端末装置の偽造に対してシステムの安全性が損われるという問題があった。

（発明が解決しようとする問題点）

本発明は、上記したように例えばICカードの偽造や端末装置の偽造に対してシステムの安全性が損われるという問題点を解決すべくなされたもので、ICカードの偽造や端末装置の偽造を防止し、システムの安全性を向上させることが可能となる相互認証方式を提供することを目的とする。

［発明の構成］

（問題点を解決するための手段）

本発明の相互認証方式は、たとえばICカード（第1の電子装置）および端末装置（第2の電子装置）にそれぞれ異なる乱数データを発生する手段を設けるとともに、ICカードおよび端末装置にそれぞれ同一の任意の入力に対して一意に定まる出力を形成する手段を設けることにより、お互いにそれぞれで発生させた乱数データを相手に送り、その送られた乱数データに対する一意に定まる出力を形成して相手に送り、送られてきた出力の内容により相手の正当性を判断し、お互いに相手が正当であると判断したときのみ通信可能にすることを特徴とする。

（作用）

ICカード（第1の電子装置）および端末装置（第2の電子装置）がお互いに相手の確認を行ない、正当と判断したときのみ通信可能にするので、ICカードの偽造や端末装置の偽造を防止でき、これによりICカードを用いたシステム全体の安全性が飛躍的に向上する。

（実施例）

以下、本発明の一実施例について図面を参照して説明する。

第3図は、本発明に係るICカード（第1の電子装置）とその上位装置である端末装置（第2の電子装置）とのシステム構成図である。

ICカード（第1の電子装置）11は、カード固有の識別番号（識別情報）ID、この識別番号IDに対応した鍵データKS、および取引口座情報などを記憶するEEPROMなどの不揮発性メモリ12、乱数データR1を発生する乱数発生部13、データの暗号化を行なう暗号化部（任意の入力に対して一意に定まる出力を形成する手段）14、後述する端末装置21と通信するためのコンタクト部15、およびこれらを制御するCPUなどの制御素子16から構成されていて、これらのうちメモリ12、乱数発生部13、暗号化部

１４および制御素子１６は、たとえば１つのＩＣチップ（あるいは複数のＩＣチップ）で構成されてＩＣカード本体内に埋設されている。

端末装置（第２の電子装置）２１は、ＩＣカード１１を取扱う機能を有し、データを記憶するメモリ２２、乱数データＲ２を発生する乱数発生部２３、データの暗号化を行なう暗号化部（任意の入力に対して一意に定まる出力を形成する手段）２４、前記鍵データＫＳと同じ鍵データを生成する鍵生成部２５、データの入力を行なうキーボード部２６、データを表示する表示部２７、ＩＣカード１１と通信するためのコンタクト部２８、およびこれらを制御するＣＰＵなどの制御部２９から構成されている。

なお、３１はＩＣカード１１と端末装置２１との間で通信するための通信回線である。また、ＩＣカード１１の暗号化部１４と端末装置２１の暗号化部２４とは、同一の暗号化アルゴリズムを有しており、暗号化に用いる入力データが同一の場合は、暗号化されて出てくる出力データも同一となる。

次に、このような構成において本発明に係る相互認証方式を第１図を用いて詳細に説明する。たとえばＩＣカード１１を用いてキャッシュレスショッピングやクレジットを行なう場合、ＩＣカード１１を端末装置２１にセットする。すると、端末装置２１の制御部２９はＩＣカード１１の制御素子１６にスタート信号Ｓを送信する。スタート信号Ｓを受信した制御素子１６は、乱数発生部１３により乱数データＲ１を発生し、その乱数データＲ１をメモリ１２に一時記憶するとともに、その乱数データＲ１およびメモリ１２内の識別番号ＩＤを端末装置２１の制御部２９に送信する。これらを受信した制御部２９は、鍵生成部２５により上記受信した識別番号ＩＤを用いてＩＣカード１１と同じ鍵データＫＳを生成し、その鍵データＫＳをメモリ２２に一時記憶する。そして、制御部２９は、暗号化部２４により上記生成した鍵データＫＳを上記受信した乱数データＲ１により暗号化することにより、暗号化された照合データＤ１１を生成し、ＩＣカード１１の制御素子１６に送信する。

照合データＤ１１を受信したＩＣカード１１の制御素子１６は、暗号化部１４によりメモリ１２に記憶されている鍵データＫＳをメモリ１２に一時記憶しておいた乱数データＲ１により暗号化することにより、暗号化された照合データＤ１２を生成する。なお、この照合データＤ１２の生成は、照合データＤ１１を受信する前にあらかじめ行なっておいてもよい。しかして、制御素子１６は、端末装置２１から受信した照合データＤ１１と内部で生成した照合データＤ１２とを比較照合し、その照合結果を端末装置２１の制御部２９に送信する。

ＩＣカード１１内の暗号化部１４および端末装置２１内の暗号化部２４は同一の暗号化アルゴリズムを有し、また乱数データＲ１は共通であり、端末装置２１が鍵生成部２５によりカード固有の鍵データＫＳを生成していれば鍵データＫＳも共通となり、Ｄ１１＝Ｄ１２となる。したがって、正当な端末装置２１であれば、ＩＣカード１１の制御素子１６において照合データＤ１１とＤ１２とを比較照合したときＤ１１＝Ｄ１２となり、照合一致の信号ＯＫを端末装置２１の制御部２９に送信する。これは、ＩＣカード１１が正当なものであるという仮定の下での例である。偽造されたＩＣカード１１であれば、比較照合の結果が照合不一致であっても、常に照合一致の信号ＯＫを送り返すようにすることが可能である。したがって、偽造されたＩＣカード１１か正当なＩＣカード１１かを端末装置２１は判断することができない。ここまでの第１の過程により、正当なＩＣカード１１は通信してよい端末装置２１か否かの判断を行ない、Ｄ１１＝Ｄ１２であれば通信可能状態とする。

ＩＣカード１１の制御素子１６から照合不一致の信号ＮＧが送信されてくると、端末装置２１の制御部２９はセットされているＩＣカード１１を排出せしめる。ＩＣカード１１の制御素子１６から照合一致の信号ＯＫが送信されてくると、端末

装置２１の制御部２９は、乱数発生部２３により乱数データＲ２を発生し、その乱数データＲ２をメモリ２２に一時記憶するとともに、その乱数データＲ２をＩＣカード１１の制御素子１６に送信する。乱数データＲ２を受信した制御素子１６は、暗号化部１４によりメモリ１２に記憶されている鍵データＫＳを上記受信した乱数データＲ２により暗号化することにより、暗号化された照合データＤ２１を生成し、端末装置２１の制御部２９に送信する。

照合データＤ２１を受信した端末装置２１の制御部２９は、暗号化部２４によりメモリ２２に一時記憶しておいた鍵データＫＳをメモリ２２に一時記憶しておいた乱数データＲ２により暗号化することにより、暗号化された照合データＤ２２を生成する。なお、この照合データＤ２２の生成は、照合データＤ２１を受信する前にあらかじめ行なっておいてもよい。しかして、制御部２９は、ＩＣカード１１から受信した照合データＤ２１と内部で生成した照合データＤ２２とを比較照合する。この照合の結果、Ｄ２１＝Ｄ２２であれば、制御部２９は端末装置２１から図示しないセンタコンピュータへの通信を可能な状態にする。Ｄ２１≠Ｄ２２であれば、制御部２９はセットされているＩＣカード１１を排出せしめる。このように、ＩＣカード１１から照合一致の信号ＯＫが送信されてきてからの第２の過程において、正当な端末装置２１は通信してよいＩＣカード１１か否かの判断を行なう。この過程によりＩＣカード１１の偽造を防止する。

このように、第１の過程においてＩＣカード１１が端末装置２１を確認し、第２の過程において端末装置２１がＩＣカード１１を確認する。その結果、お互いに相手を正当と認めたときのみ通信可能状態、すなわちデータの交換あるいはデータの読み書きを可能にする。これにより、個人データやシステム固有のデータなどを保護し、システム全体のセキュリティを向上させる。

なお、ＩＣカード１１および端末装置２１の両方が偽造された場合、センタコンピュータが端末装置２１の正当性確認を前記第１の過程のように行なえば、システムのセキュリティは更に向上する。

また、上記実施例では、ＩＣカード１１がまず端末装置２１を確認したが、その逆も可能である。第２図はその一例を示し、第１図の場合と同様にして相互認証が可能である。

さらに、第２の電子装置がＩＣカードを発行するためのＩＣカード発行装置であって、ＩＣカードを発行する際にも本発明の相互認証方式を適用することが可能である。

ここで、端末装置２１の鍵生成部２５における鍵データＫＳの生成方法としては、たとえば識別番号ＩＤを論理的にシフトさせたり、排他的論理和をとったものでもよく、識別番号ＩＤからカード固有の鍵データＫＳを得られるものであればよい。あるいは、識別番号ＩＤおよびカード固有の鍵データＫＳのファイルを内蔵していてもよい。

第４図は鍵データＫＳを生成する生成方法の一例を示し、以下それについて簡単に説明する。たとえば同図（ａ）に示すような１桁が４ビットからなる１６桁の識別番号ＩＤを、同図（ｂ）に示すように変換（ビットの並べ変え）した後、同図（ｃ）に示すようなビットの位置変えをした識別番号ＩＤ′を生成する。そして、同図（ｄ）（ｅ）に示すように、識別番号ＩＤ′の先頭の１バイトの値だけを最後尾にシフトさせて鍵データＫＳとするものである。

また、乱数発生部１３，２３は相異なるものがよい。お互いに独立しているものであり、かつ時間的関数がよい。時間的関数としては、たとえば内蔵した時計機能の時刻データや内部で発生されるクロックパルスを分周したものを用いる。

以上説明したような相互認証方式によれば、ＩＣカードおよび端末装置がお互いに相手の確認を行ない、正当と判断したときのみ通信可能にするので、ＩＣカードの偽造や端末装置の偽造を防止できる。これにより、ＩＣカードを用いたシステム全体の安全性が飛躍的に向上する。

【発明の効果】

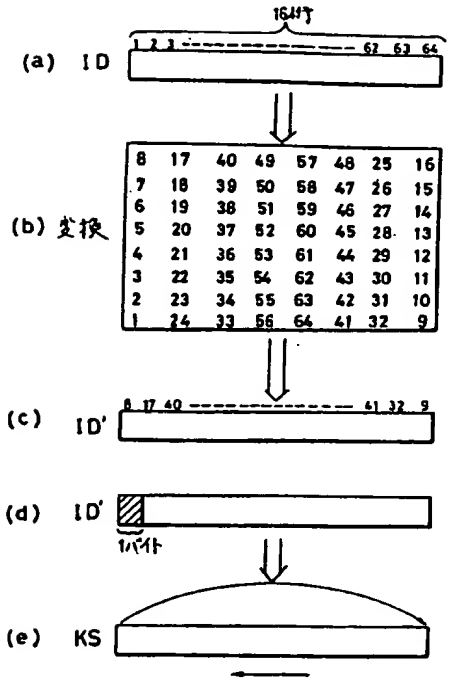
以上詳述したように本発明によれば、ＩＣカードの偽造や端末装置の偽造を防止し、システムの安全性を向上させることが可能となる相互認証方式を提供できる。

４．図面の簡単な説明

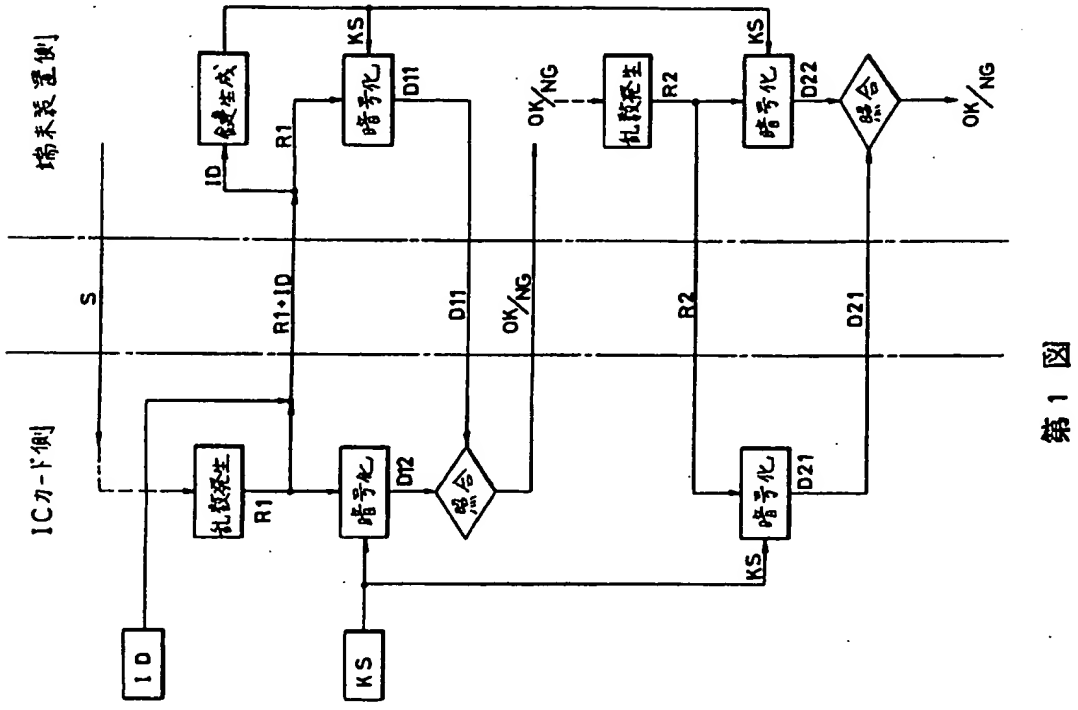
図は本発明の一実施例を説明するためのもので、第１図および第２図は相互認証方式を説明する流れ図、第３図はＩＣカードと端末装置とのシステム構成図、第４図は鍵生成部における鍵データの生成方法を説明する図である。

１１……ＩＣカード（第１の電子装置）、１２……不揮発性メモリ、１３……乱数発生部、１４……暗号化部、１５……コンタクト部、１６……制御素子、２１……端末装置（第２の電子装置）、２２……メモリ、２３……乱数発生部、２４……暗号化部、２５……鍵生成部、２６……キーボード部、２７……表示部、２８……コンタクト部、２９……制御部、３１……通信回線。

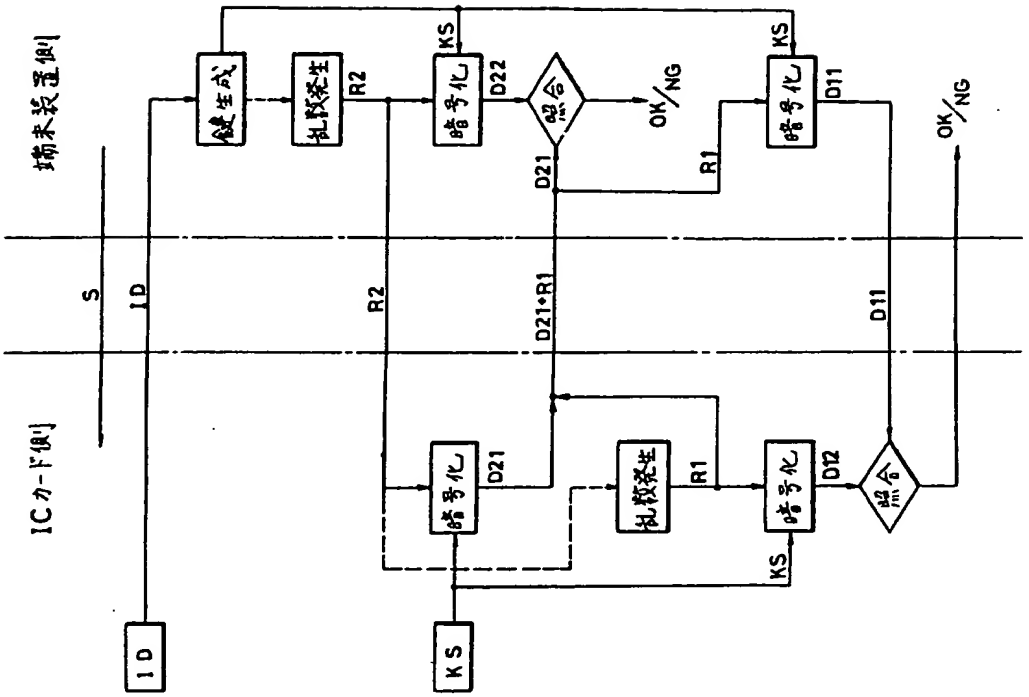
出願人代理人　弁理士　鈴江武彦



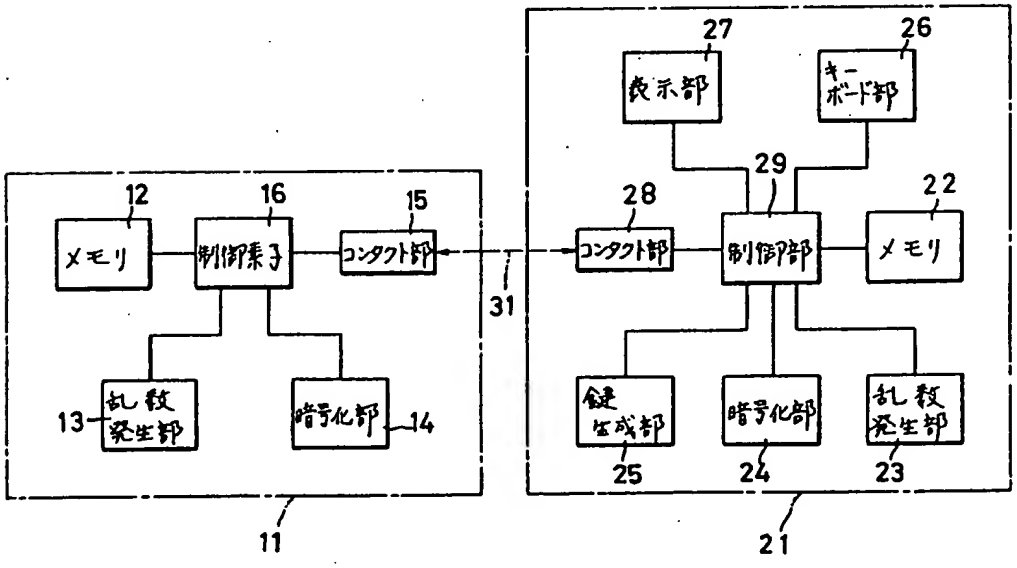
第４図



第１図


端末装置側
ICカード側
S
ID
鍵生成
乱数発生
R2
暗号化
D22
照合
OK/NG
KS
D21
R1
暗号化
D11
OK/NG
D21・R1
D11
暗号化
D21
乱数発生
R1
暗号化
D12
照合
KS
ID
KS

第2図


27
表示部
26
キーボード部
29
28
22
12
16
15
メモリ
制御素子
コンタクト部
コンタクト部
制御部
メモリ
31
13
乱数発生部
暗号化部
14
鍵生成部
暗号化部
乱数発生部
25
24
23
11
21

第3図